INTRODUCTION: GIAC ENTERPRISES

- World’s largest supplier of fortune-cookie sayings
- E-commerce site for fortune orders
- Cookie sayings submission via mobile app; stored in MySQL Database that is highest value asset
- Log volume is too high for manual analysis, need low-cost SIEM solution
PROJECT OVERVIEW

Product Selection

Product Implementation

Product Testing

Final Acceptance
GIAC ARCHITECTURE

- Two datacenters, each with:
  - Apache web servers
  - MySQL database backend
  - HAProxy
  - Web Application Firewall
  - Cisco Firewall and Switches/Routers
  - Mobile Device Management for employee/contractor BYOD
  - Active Directory Infrastructure
- Employee/contractors:
  - Primarily Windows desktops
  - Contractor-owned systems for fortune submission
IMPORTANT FEATURES

• Windows and Linux log support
• Active open source community
• Log correlation
• Threat Feeds
• Role-based Access Control
• Long-term log storage
INSTALLATION & CONFIGURATION

• Installs from ISO image
  • Conversion process for use in AWS
  • Setup configures interfaces and initial accounts

• Wizard for easy configuration
  • Initial asset & network discovery
DATA SOURCES

- Windows Event Logs
- OSSEC Rootkit Detection & File Change Monitoring
- Linux Syslog
- Apache Logs
- Database Logs
- Vulnerability Scans
- Open Threat Exchange
- NMAP
LOGGING CONFIGURATION

- Log data parsed & normalized via plugins
- Most can be configured via wizard or web interface
- Some require console “Jailbreak” to enable
  - Rsyslog
  - Database plugins
VULNERABILITY SCANS

- Can be run ad-hoc or scheduled
- Configured to run against specific asset group
- Credentialed & Unauthenticated
- Built-in default scans or full customization of checks
OPEN THREAT EXCHANGE

• OTX “Pulses” contain community-updated source of current threat data

• Can subscribe to single Pulse or user feed

• Pulses Contain Indicators of Compromise
  • IP addresses, URLs, domain data
  • File hashes
  • Geographical data

• Tagged by OS, software

<table>
<thead>
<tr>
<th>TOP 10 COUNTRIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
</tr>
<tr>
<td>China</td>
</tr>
<tr>
<td>Switzerland</td>
</tr>
<tr>
<td>Russian Federation</td>
</tr>
<tr>
<td>Netherlands</td>
</tr>
<tr>
<td>France</td>
</tr>
<tr>
<td>Ukraine</td>
</tr>
<tr>
<td>United Kingdom</td>
</tr>
<tr>
<td>Lithuania</td>
</tr>
<tr>
<td>United States</td>
</tr>
<tr>
<td>South Korea</td>
</tr>
</tbody>
</table>
TICKET SYSTEM

• Opened automatically for vulnerabilities or alarms above a configured severity threshold
• Can be updated, re-assigned, and have status or priority changed
• Ability to close as false positives
STRENGTHS AND WEAKNESSES

• Supports many of GIAC’s data sources out of the box
• Highly configurable; allows customized plugins, rules, severities
• Good documentation and online support resources
• Vulnerability scanning with update
• HIDS capabilities

• Resource-intensive; requires lots of memory and CPU to support
• Open Threat Exchange potentially powerful capability, but not easy to use well
• Limited reporting capabilities
NEXT STEPS

• Configure TLS for log sources
• Add ELK stack for long-term log storage
• Tune logs and alerting:
  • to reduce false positives
  • improve performance
• Create plugins for unsupported sources
• Investigate active-response capabilities
CONCLUSION

• Successful Proof of Concept, should move forward with full deployment
  • Supports major GIAC use cases out of the box
  • Potential solution for long-term log storage
  • Highly flexible system
  • Enterprise solution available if support needed
<table>
<thead>
<tr>
<th>SANS OnDemand</th>
<th>OnlineUS</th>
<th>Anytime</th>
<th>Self Paced</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>